

10/521858

Secure authenticated distance measurement

The invention relates to a method for a first communication device to performing authenticated distance measurement between a first communication device and a second communication device. The invention also relates to a method of determining whether data stored on a first communication device is to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

Digital media have become popular carriers for various types of data information. Computer software and audio information, for instance, are widely available on optical compact disks (CDs) and recently also DVD has gained in distribution share. The CD and the DVD utilize a common standard for the digital recording of data, software, images, and audio. Additional media, such as recordable discs, solid-state memory, and the like, are making considerable gains in the software and data distribution market.

The substantially superior quality of the digital format as compared to the analog format renders the former substantially more prone to unauthorized copying and pirating, further a digital format is both easier and faster to copy. Copying of a digital data stream, whether compressed, uncompressed, encrypted or non-encrypted, typically does not lead to any appreciable loss of quality in the data. Digital copying thus is essentially unlimited in terms of multi-generation copying. Analog data with its signal to noise ratio loss with every sequential copy, on the other hand, is naturally limited in terms of multi-generation and mass copying.

The advent of the recent popularity in the digital format has also brought about a slew of copy protection and DRM systems and methods. These systems and methods use technologies such as encryption, watermarking and right descriptions (e.g. rules for accessing and copying data).

One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if

- the receiving device has been authenticated as being a compliant device,
- if the user of the content has the right to transfer (move, copy) that content to another device.

If transfer of content is allowed, this will typically be performed in an encrypted way to make sure that the content cannot be captured illegally in a useful format.

Technology to perform device authentication and encrypted content transfer is available and is called a secure authenticated channel (SAC). Although it might be allowed to make copies of content over a SAC, the content industry is very bullish on content distribution over the Internet. This results in disagreement of the content industry on transferring content over interfaces that match well with the Internet, e.g. Ethernet.

Further, it should be possible for a user visiting his neighbour to watch a movie, which he owns, on the neighbour's big television screen. Typically, the content owner will disallow this, but it might become acceptable if it can be proved that a license holder of that movie (or a device that the license holder owns) is near that television screen.

It is therefore of interest to be able to include an authenticated distance measurement when deciding whether content should be accessed or copied by other devices.

In the article by Stefan Brands and David Chaum, "Distance-Bounding protocols", Eurocrypt '93 (1993), Pages 344-359, integration of distance-bounding protocols with public-key identification schemes is described. Here distance measurement is described based on time measurement using challenge and response bits and with the use of a commitment protocol. This does not allow authenticated device compliancy testing and is not efficient when two devices must also authenticate each other.

It is an object of the invention to obtain a solution to the problem of performing a secure transfer of content within a limited distance.

This is obtained by a method for a first communication device to performing authenticated distance measurement between said first communication device and a second communication device, wherein the first and the second communication device share a common secret and said common secret is used for performing the distance measurement between said first and said second communication device.

Because the common secret is being used for performing the distance measurement, it can be ensured that when measuring the distance from the first communication device to the second communication device, it is the distance between the right devices that is being measured.

The method combines a distance measurement protocol with an authentication protocol. This enables authenticated device compliancy testing and is efficient, because a secure channel is anyhow needed to enable secure communication between devices and a device can first be tested on compliancy before a distance measurement is executed.

In a specific embodiment, the authenticated distance measurement is performed according to the following steps,

- transmitting a first signal from the first communication device to the second communication device at a first time t_1 , said second communication device being adapted for receiving said first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device,
- receiving the second signal at a second time t_2 ,
- checking if the second signal has been modified according to the common secret,
- determining the distance between the first and the second communication device according to a time difference between t_1 and t_2 .

When measuring a distance by measuring the time difference between transmitting and receiving a signal and using a secret, shared between the first and the second communication device, for determining whether the returned signal really originated from the second communication device, the distance is measured in a secure authenticated way ensuring that the distance will not be measured to a third communication device (not knowing the secret). Using the shared secret for modifying the signal is a simple way to perform a secure authenticated distance measurement.

In a specific embodiment the first signal is a spread spectrum signal. Thereby a high resolution is obtained and it is possible to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In another embodiment the step of checking if the second signal has been modified according to the common secret is performed by the steps of,

- generating a third signal by modifying the first signal according to the common secret,
- comparing the third signal with the received second signal.

This method is an easy and simple way of performing the check, but it requires that both the first communication device and the second communication device know how the first signal is being modified using the common secret.

In a specific embodiment the first signal and the common secret are bit words and the second signal comprises information being generated by performing an XOR between the bit words. Thereby, it is a very simple operation that has to be performed, resulting in demand for few resources by both the first and the second communication device when performing the operation.

In an embodiment the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,

- performing an authentication check from the first communication device on the second communication device by checking whether said second communication device is compliant with a set of predefined compliance rules,
- if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device.

This is a secure way of performing the sharing of the secret, ensuring that only devices being compliant with compliance rules can receive the secret. Further, the shared secret can afterwards be used for generating a SAC channel between the two devices. The secret could be shared using e.g. key transport mechanisms as described in ISO 11770-3. Alternatively, a key agreement protocol could be used, which e.g. is also described in ISO 11770-3.

In another embodiment the authentication check further comprises checking if the identification of the second device is compliant with an expected identification. Thereby, it is ensured that the second device really is the device that it should be. The identity could be obtained by checking a certificate stored in the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between the first and the second communication device and checking whether said measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. By using the authenticated distance measurement in connection with sharing data between devices, unauthorised distribution of content can be reduced.

In a specific embodiment the data stored on the first device is sent to the second device if it is determined that the data stored on the first device are to be accessed by the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between a third communication device and the second communication device and checking whether said measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. In this embodiment, the distance is not measured between the first communication device, on which the data are stored, and the second communication device. Instead, the distance is measured between a third communication device and the second communication device, where the third communication device could be personal to the owner of the content.

The invention also relates to a communication device for performing authenticated distance measurement to a second communication device, where the communication device shares a common secret with the second communication device and where the communication device comprises means for measuring the distance to the second device using said common secret.

In an embodiment the device comprises,

- means for transmitting a first signal to a second communication device at a first time t_1 , said second communication device being adapted for receiving said first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal,
- means for receiving the second signal at a second time t_2 ,
- means for checking if the second signal has been modified according to the common secret,
- means for determining the distance between the first and the second communication device according to a time difference between t_1 and t_2 .

The invention also relates to an apparatus for playing back multimedia content comprising a communication device according to the above.

In the following preferred embodiments of the invention will be described referring to the figures, wherein

Figure 1 illustrates authenticated distance measurement being used for content protection,

Figure 2 is a flow diagram illustrating the method of performing authenticated distance measurement,

Figure 3 illustrates in further detail the step of performing the authenticated distance measurement shown in figure 2,

Figure 4 illustrates a communication device for performing authenticated distance measurement.

Figure 1 illustrates an embodiment where authenticated distance measurement is being used for content protection. In the centre of the circle 101 a computer 103 is placed. The computer comprises content, such as multimedia content being video or audio, stored on e.g. a hard disk, DVD or a CD. The owner of the computer owns the content and therefore the computer is authorised to access and present the multimedia content for the user. When the user wants to make a legal copy of the content to another device via e.g. a SAC, the distance between the other device and the computer 103 is measured and only devices within a predefined distance illustrated by the devices 105, 107, 109, 111, 113 inside the circle 101 are allowed to receive the content. Whereas the devices 115, 117, 119 having a distance to the computer 101 being larger than the predefined distance are not allowed to receive the content.

In the example a device is a computer, but it could e.g. also be a DVD drive, a CD drive or a Video, as long as the device comprises a communication device for performing the distance measurement.

In a specific example the distance might not have to be measured between the computer, on which the data are stored, and the other device, it could also be a third device e.g. a device being personal to the owner of the content which is within the predefined distance.

In figure 2 a flow diagram illustrates the general idea of performing authenticated distance measurement between two devices, 201 and 203 each comprising communication devices for performing the authenticated distance measurement. In the example the first device 201 comprises content which the second device 203 has requested. The authenticated distance measurement then is as follows. In 205 the first device 201 authenticates the second device 203; this could comprise the steps of checking whether the

second device 203 is a compliant device and might also comprise the step of checking whether the second device 203 really is the device identified to the first device 201. Then in 207, the first device 201 exchanges a secret with the second device 203, which e.g. could be performed by transmitting a random generated bit word to 203. The secret should be shared securely, e.g. according to some key management protocol as described in e.g. ISO 11770.

Then in 209, a signal for distance measurement is transmitted to the second device 203; the second device modifies the received signal according to the secret and retransmits the modified signal back to the first device. The first device 201 measures the round trip time between the signal leaving and the signal returning and checks if the returned signal was modified according to the exchanged secret. The modification of the returned signal according to some secret will most likely be dependent on the transmission system and the signal used for distance measurement, i.e. it will be specific for each communication system (such as 1394, Ethernet, Bluetooth, IEEE 802.11, etc.).

The signal used for the distance measurement may be a normal data bit signal, but also special signals other than for data communication may be used. In an embodiment spread spectrum signals are used to be able to get high resolution and to be able to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In a specific example a direct sequence spread spectrum signal is used for distance measurement; this signal could be modified by XORing the chips (e.g. spreading code consisting of 127 chips) of the direct sequence code by the bits of the secret (e.g. secret consists also of 127 bits). Also, other mathematical operations as XOR could be used.

The authentication 205 and exchange of secret 207 could be performed using the protocols described in some known ISO standards ISO 9798 and ISO 11770. For example the first device 201 could authenticate the second device 203 according to the following communication scenario:

First device -> Second device: $R_B || \text{Text 1}$

where R_B is a random number

Second device -> First device: $\text{CertA} || \text{TokenAB}$

Where CertA is a certificate of A

$\text{TokenAB} = R_A || R_B || B || \text{Text3} || s_A(R_A || R_B || B || \text{Text2})$

R_A is a random number

Identifier B is an option

sS_A is a signature set by A using private key S_A

If TokenAB is replaced with the token as specified in ISO 11770-3 we at the same time can do secret key exchange. We can use this by substituting Text2 by:

$\text{Text2} := eP_B(A || K || \text{Text2}) || \text{Text3}$

Where eP_B is encrypted with Public key B

A is identifier of A

K is a secret to be exchanged

In this case the second device 203 determines the key (i.e. has key control), this is also called a key transport protocol, but also a key agreement protocol could be used. This may be undesirable in which case it can be reversed, such that the first device determines the key. A secret key has now been exchanged according to 207 in figure 2. Again, the secret key could be exchanged by e.g. a key transport protocol or a key agreement protocol.

After the distance has been measured in a secure authenticated way as described above content, data can be send between the first and the second device in 211.

Figure 3 illustrates in further detail the step of performing the authenticated distance measurement. As described above the first device 301 and the second device 303 have exchanged a secret; the secret is stored in the memory 305 of the first device and the memory 307 of the second device. In order to perform the distance measurement, a signal is transmitted to the second device via a transmitter 309. The second device receives the signal via a receiver 311 and 313 modifies the signal by using the locally stored secret. The signal is modified according to rules known by the first device 301 and transmitted back to the first device 301 via a transmitter 315. The first device 301 receives the modified signal via a receiver 317 and in 319 the received modified signal is compared to a signal, which has been modified locally. The local modification is performed in 321 by using the signal transmitted to the second device in 309 and then modifying the signal using the locally stored secret similar to the modification rules used by the second device. If the received modified signal and the locally modified signal are identical, then the received signal is authenticated and can be used for determining the distance between the first and the second device. If the two

signals are not identical, then the received signal cannot be authenticated and can therefore not be used for measuring the distance as illustrated by 325. In 323 the distance is calculated between the first and the second device; this could e.g. be performed by measuring the time, when the signal is transmitted by the transmitter 309 from the first device to the second device and measuring when the receiver 317 receives the signal from the second device. The time difference between transmittal time and receive time can then be used for determining the physical distance between the first device and the second device.

In figure 4 a communication device for performing authenticated distance measurement is illustrated. The device 401 comprises a receiver 403 and a transmitter 411. The device further comprises means for performing the steps described above, which could be by executing software using a microprocessor 413 connected to memory 417 via a communication bus. The communication device could then be placed inside devices such as a DVD, a computer, a CD, a CD recorder, a television and other devices for accessing protected content.